IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MATT DAVIS, LAKIA MORTON, and ZACHARY CHERNIK, individually and on behalf of all others similarly situated, Plaintiffs, v. SAMSUNG ELECTRONICS AMERICA, INC., Defendant.	Case No.: _____ **COMPLAINT—CLASS ACTION** **DEMAND FOR JURY TRIAL**

Plaintiffs, Matt Davis, Lakia Morton, and Zachary Chernik ("Plaintiffs"), individually and on behalf of all others similarly situated, through the undersigned counsel below, hereby allege the following against Defendant Samsung Electronics America, Inc. ("Samsung" or "Defendant"). Based upon personal knowledge as to their own actions, and upon information, belief, and investigation of counsel as to all other matters, Plaintiffs specifically allege as follows:

SUMMARY OF THE CASE

1. Plaintiffs bring this class action on behalf of a nationwide class, a Georgia sub-class, and an Illinois sub-class (together, the "Classes") against Samsung for its failure to properly secure and safeguard the sensitive and

confidential personally identifiable information, including names, addresses, telephone numbers, email addresses, dates of birth and other sensitive information (collectively, "personally identifiable information" or "PII"), of millions of its current and former customers ("Class Members").

2. In July 2022, a large quantity of PII entrusted to Samsung by its customers was exfiltrated and stolen by an unauthorized third party (the "Data Breach"). Only a few months earlier, in March 2022, Samsung had confirmed another data security breach; at that time, an organization called Lapsus$ accessed and stole Samsung's confidential data and published 190GBs of Samsung's confidential data online.

3. Despite this earlier breach and knowledge of the exposed sensitive technical data and the immediate need to protect customers' PII from attackers, Samsung utterly failed to adequately secure its systems and allowed another breach to occur, this time compromising consumer PII.

4. Plaintiffs and Class Members entrusted Samsung with their sensitive and valuable PII. Even more egregious, there was absolutely no need for Samsung to collect this PII from purchasers of its electronic devices or other appliances. Samsung did so to increase its profits, to gather information regarding its

customers to be able to track its customers and their behaviors, and to use the data for its own benefit and purposes.

5. Plaintiffs and Class Members could not have expected that purchasing an electronic device or home appliance and registering for an account in connection with the purchase, which was required by Samsung to access features of the devices, would lead to such a devastating loss and continuing risk of injury for years following the purchase.

6. By collecting, using, selling, monitoring, and trafficking Plaintiffs' and other Class Members' PII for its own economic benefit, and utterly failing to protect it, including by maintaining inadequate security systems, failing to properly archive the PII, allowing access by third parties and failing to implement sufficient security measures, Samsung has caused harm to Plaintiffs and Class Members.

7. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect its customers' PII; (ii) warn customers of its inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct constitutes negligence that proximately caused damages to Plaintiffs and Class Members as alleged herein.

8. Samsung disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that its customers' PII was safeguarded; failing to take available steps to prevent unauthorized disclosure of data; and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

9. Alternatively, Defendant has been unjustly enriched. The amounts Plaintiffs and Class Members paid for Defendant's goods and services should have been used, in part, to pay for the administrative costs of data management and security, including the proper and safe disposal of Plaintiffs' and Class Members' PII. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement the data management and security measures mandated by industry standards.

10. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII, a form of property that Samsung obtained from Plaintiffs and Class Members; (ii)

increased out-of-pocket expenses associated with identity defense, credit monitoring services and other prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; and (v) violation of Plaintiffs' and Class Members' privacy rights.

11. As a direct and proximate result of Samsung's breach of confidence and duties and also Samsung's failure to protect their PII, Plaintiffs and Class Members have been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuses of their PII; ongoing monetary loss and economic harm; loss of value of privacy and confidentiality of the stolen PII; illegal sales of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring; identity theft insurance costs; credit freezes/unfreezes; expenses and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost work time and other injuries. Plaintiffs

and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as Plaintiffs are citizens of Illinois and Georgia (and the proposed class members are from various states) while Defendant is a citizen of New York and New Jersey; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

13. This Court has personal jurisdiction over Defendant because Defendant transacts substantial business in this District, has substantial aggregate contacts with this District, and purposefully availed itself of the laws of Georgia in this District, because the acts and transactions giving rise to this action occurred in this District.

14. Pursuant to 28 U.S.C. § 1391, venue is proper in this District because a substantial part of the events, omissions, and acts giving rise to Plaintiffs' claims herein occurred in this District.

THE PARTIES

15. Plaintiff Matt Davis is a citizen and resident of the State of Georgia and is a current Samsung customer who had his PII exfiltrated and compromised in the Data Breach.

16. Plaintiff Davis owns numerous Samsung products where he submitted his PII to Samsung, including his name, email, date of birth, and zip code. These products include:

- Numerous mobile phones, including the Galaxy Note, Galaxy Note 2, Galaxy Note 4, Galaxy Note 5, Galaxy Note 6, Galaxy Note 7, Galaxy Note 10, Galaxy S21 and Galaxy S22 Ultra;
- A smart television purchased in 2017;
- A Galaxy Book Pro 360 laptop purchased in 2020;
- A home automation system SmartThings Hub purchased and installed for at least 6 years; and
- Home appliances, including a washer, dryer, and refrigerator.

17. In making his decision to create a Samsung account to gain full access to the product's features, Plaintiff Davis reasonably expected that Samsung would safeguard his PII.

18. Since the announcement of the Data Breach, Plaintiff Davis has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII—time which he would not have had to expend but for the Data Breach.

19. As a direct and proximate result of the Data Breach, Plaintiff Davis has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to conducting research concerning the Data Breach and reviewing credit reports and financial account statements for any indication of actual or attempted identity theft or fraud. This is valuable time that Plaintiff Davis could have spent on other activities.

20. As a result of the Data Breach, Plaintiff Davis will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages, for years to come.

21. Plaintiff Lakia Morton is a citizen and resident of the State of Georgia and is a current Samsung customer who had her PII exfiltrated and compromised in the Data Breach.

22. Plaintiff Morton owns numerous Samsung products where she submitted her PII to Samsung, including her name, email, date of birth, and zip code. These products include:

- A 75" Smart television purchased in 2019;
- Multiple pairs of Galaxy Buds Pro purchased in 2020 and 2021;
- A Galaxy Note phone purchased in 2019; and
- A front load washer and dryer purchased in 2020.

23. In making her decision to create a Samsung account to gain full access to the product's features, Plaintiff Lakia Morton reasonably expected that Samsung would safeguard her PII.

24. Since the announcement of the Data Breach, Plaintiff Morton has been required to spend her valuable time monitoring her various accounts in an effort to detect and prevent any misuses of his PII—time which she would not have had to expend but for the Data Breach.

25. As a direct and proximate result of the Data Breach, Plaintiff Morton has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to conducting research concerning the Data Breach and reviewing credit reports and financial account statements for any indication of actual or attempted identity theft or fraud. This is valuable time that Plaintiff Morton could have spent on other activities.

26. As a result of the Data Breach, Plaintiff Morton will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages, for years to come.

27. Plaintiff Zachary Chernik is a citizen and resident of the State of Illinois and is a current Samsung customer who had his PII exfiltrated and compromised in the Data Breach.

28. Plaintiff Chernik purchased a Samsung S7 Cell Phone from Verizon on or about June 22, 2016. As part of his purchase he was required to, and did, submit his PII to Samsung, including his name, email, date of birth, and zip code.

29. In making his decision to create a Samsung account to gain full access to the product's features, Plaintiff Chernik reasonably expected that Samsung would safeguard his PII.

30. Since the announcement of the Data Breach, Plaintiff Chernik has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII—time which he would not have had to expend but for the Data Breach.

31. As a direct and proximate result of the Data Breach, Plaintiff Chernik has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to conducting research concerning the Data Breach and reviewing

credit reports and financial account statements for any indication of actual or attempted identity theft or fraud. This is valuable time that Plaintiff Chernik could have spent on other activities.

32. As a result of the Data Breach, Plaintiff Chernik will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages, for years to come.

33. Samsung is a corporation incorporated in the State of New York, with its United States headquarters and principal place of business located at 85 Challenger Road, Ridgefield, New Jersey 07660-2118.

34. Defendant Samsung Electronics America, Inc. is a United States-based subsidiary of Samsung Electronics Co., Ltd, and is responsible for the production and sale of billions of dollars of electronics sold in the United States.

35. Defendant maintains offices and employees who specifically oversee and handle data privacy, data policies and make data-driven decisions. The Samsung "Privacy Office" is located at 85 Challenger Road, Ridgefield Park, NJ 07660, NAPrivacy@sea.samsung.com.[1]

[1] *See* https://account.samsung.com/membership/terms/privacypolicy (last accessed Dec. 6, 2022).

FACTUAL ALLEGATIONS

36. Defendant Samsung purports to be an industry leader in technology. It is a technology and electronics giant that sells millions of products and produces over $240 billion of revenue each year. It produces a wide array of electronic devices but is best known for being a top manufacturer of mobile phones, smartphones, televisions, semiconductor chips, tablets, laptops, and home appliances.

37. Samsung's televisions and home appliances connect to the internet and require customers to create a "Samsung Account" prior to accessing many of their device's features. For example, consumers who purchase Samsung "smart" televisions often do so to watch streaming applications such as Netflix or Hulu on a television. An owner of a Samsung smart television cannot access the streaming applications without downloading those applications onto their television. In order to download the applications, the owner of the Samsung smart television must first create a Samsung Account.

38. In fact, for nearly all of its products and services, Samsung requires that the customer create a Samsung Account, forcing customers to entrust Samsung with their PII in order to use the products and services. In fact, regardless of whether the customer purchased a printer, television, smartphone, refrigerator, or

laptop, the customer needs to register the products with Samsung to access the features of the devices. Consumers are therefore forced to register accounts; otherwise, many product features are locked and inaccessible. Even using the products in the way they are intended to be used is nearly impossible without the required registration.

39. Samsung requires customers to register the product purchased for warranty-related purposes and to access certain drivers and software needed for the products. These features are essential to the function of the devices.

40. Many features advertised and promoted by Samsung with the sale of the products can only be accessed after the customer creates a Samsung Account. By locking features, making software updates otherwise inaccessible and blocking intended uses of the products, Samsung ensures that nearly every customer who purchases a Samsung product, at some point, will be forced to submit their PII through product registration and creation of the Samsung Account.

41. Other product-related benefits cannot be accessed without a Samsung account. These benefits include, but are not limited to, product support, order tracking, exclusive rewards and offers, Samsung Rewards, Galaxy Store, Samsung Pay, Samsung Health, Samsung Members and Samsung TV Plus.

42. The information collected and stored by Samsung includes, but is not limited to names, dates of birth, mailing addresses, email addresses, phone numbers, payment card information, precise geolocation data and information about the product the customer purchased.

43. In addition to the information inputted by the customer for the Samsung Account, Samsung also collects still more information automatically from its customers concerning their Samsung devices, such as their mobile network operator; connections to other devices; application usage information; the username and password for participating third party devices, apps, features, and services; device settings; websites visited; search terms used; which applications, services or features the customer downloaded or purchased; and how and when the applications and services are used.[2]

44. Defendant holds itself out as a trustworthy company that recognizes and values the customer's privacy and personal information. Samsung's Privacy Policy for the U.S. assures its customers that Samsung "maintain[s] safeguards designed to protect personal information we obtain through the Services."

[2] *Samsung Privacy Policy for the U.S.*, Samsung (last updated Oct. 1, 2022), https://www.samsung.com/us/account/privacy-policy/.

Samsung represented that it has "industry-leading security" and that "security and privacy are at the core of what we do and what we think about every day."[3]

45. Samsung's privacy policy and online advertisements clearly and unequivocally provide that any personal information provided to Samsung will remain secure and protected. Samsung says "We maintain safeguards designed to protect personal information we obtain through the Services," and purports to use the personal information it collects from users to "protect against, identify, and prevent fraud and other criminal activity."[4] Samsung asserts it "take[s] data security very seriously."[5] Samsung "products are designed to keep [] data private and secure while always pushing forward to offer [] the latest, most groundbreaking innovation."[6]

46. Plaintiffs and other Class Members relied to their detriment on Samsung's representations and were harmed by Samsung's omissions regarding data security, including Samsung's failure to alert customers that its security protections were inadequate and that Defendant would forever store the customers' PII, fail to archive it, fail to protect it, and fail to warn customers of the anticipated and foreseeable data breach.

---

[3] *Id.*
[4] *Id.*
[5] *Samsung's Privacy Principles*, Samsung, https://www.samsung.com/us/privacy/
[6] *Id.*

47. Had Samsung disclosed to Plaintiffs and Class Members that its data systems were not secure at all and were vulnerable to attack, Plaintiffs would not have purchased Samsung's products or utilized its services that led to the account creation. Thus, Plaintiffs and Class Members significantly overpaid based on what the products were represented to be compared to what Plaintiffs and Class Members actually received.

48. To reduce the likelihood of data breaches like that which occurred here, the Federal Trade Commission ("FTC") has established security guidelines and recommendations for businesses like Samsung that possess their customers' sensitive PII. Among such recommendations are limiting the sensitive consumer information companies keep, encrypting sensitive information sent to third parties or stored on computer networks, and identifying and understanding network vulnerabilities.

49. Thus, Samsung had obligations created by contract, industry standards, common law, and its privacy policies and representations to its customers to keep PII confidential and protect it from unauthorized disclosures exactly like that which occurred in the Data Breach.

50. Samsung enriched itself through the collection of a treasure trove of sensitive PII from Plaintiffs and Class Members and profited from the collection,

yet it failed to use some of those profits to employ reasonable, accepted safety measures to secure this valuable information.

51. On September 2, 2022, Samsung released a statement that its "U.S. systems" had be infiltrated in "late July 2022" by an "unauthorized third party" and PII including at least customer names, contact, and demographic information, date of birth and product registration information had been stolen.

52. According to Samsung, the breach was not discovered until "around August 4, 2022" after an "ongoing investigation." Samsung did not disclose the breach to the affected customers for almost a month.

53. Samsung's carefully worded statement did not explain how the data breach occurred; how the breach was discovered; what systems were affected; why it took almost a month to disclose the breach; the number of Samsung customers affected; how long the investigation had been ongoing; the number of years of data involved; the volume of data accessed; what specific demographic data was stolen; the exact extent of the PII that was stolen; or whether this Data Breach was related to an earlier data breach of Samsung internal data.

54. Cybersecurity industry experts viewed the statement that was issued late on a Friday evening before the Labor Day holiday weekend, the failure to

disclose the number of individuals impacted by the breach, and the month-long delay, as Samsung's attempt to minimize the incident.

55. In its Data Breach notice, Samsung assures its customers that "no immediate action [is] necessary for any of Samsung's platforms," but nevertheless recommends that impacted customers: (1) "[r]emain cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information"; (2) "[a]void clicking on links or downloading attachments from suspicious emails"; and (3) "review [] accounts for suspicious activities."

56. Despite its failure to protect its customers highly personal data, Samsung did not offer impacted customers identity theft protection services. Rather, Samsung merely reminded customers that they are entitled to one free credit report from one of the three major credit reporting agencies.

57. Earlier, on March 7, 2022, Samsung announced it had suffered a data breach that exposed only internal company data, including the source code related to its Galaxy smartphones, algorithms related to Samsung smartphone biometric authentication, bootloader source code to bypass some of Samsung's operating system controls, source code for Samsung's activation servers and full source for technology used for authorizing and authenticating Samsung accounts.

58. Samsung claimed that the data breach did not include the PII of consumers or Samsung employees.

59. The breach came to light after the hacking group Lapsus$ disclosed 190GBs of Samsung's data to 400 peers.

60. Following the data breach, Samsung promised that it would implement measures to prevent further incidents and would continue to serve its customers without disruption.

61. It is possible that the Data Breach announced on September 2, 2022 is a continuation of the data breach announced on March 7, 2022. Given the difficulty of completely eliminating malware once it has infiltrated a network as large and complex as Samsung's, and the delay in disclosing the breach to the public, cybersecurity industry expert Chad McDonald has expressed the opinion that "this was quite likely just a continuation of [the earlier breach] they just hadn't discovered yet."

62. Even if the prior March 2022 data breach and the Data Breach are separate and distinct events, Samsung's repeated data security failures and deficient notice evince a reckless disregard for maintaining adequate data security to protect Plaintiffs' and the Class Member's PII from exposure, compromise, and/or exfiltration by cyber-criminals.

63. Plaintiffs and other Class Members have been injured by the disclosure of their PII in the Data Breach.

64. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name. As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

65. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconvenience repairing damage to their credit records" and their "good name."

66. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud.

67. There may be a time lag between when PII is stolen and when it is used. According to the GAO Report: [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the

Web, fraudulent use of that information may continue for years.[7] As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

68. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[9]

69. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches,

---

[7] *See* Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007), United States Government Accountability office, available at https://www.gao.gov/new.items/d07737.pdf.

[8] *Id*. at 29.

[9] *See* Federal Trade Commission, WARNING SIGNS OF IDENTIFY THEFT, available at https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.

identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other PII directly on various Internet websites making the information publicly available.

CLASS ALLEGATIONS

70. Under Rule 23, Plaintiffs brings this case as a class action on behalf of a Nationwide Class, and Georgia and Illinois State Sub-Classes, defined as follows:

> **Nationwide Class**: All persons in the United States whose PII was maintained on the Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.
>
> **Georgia Sub-Class**: All persons in the State of Georgia whose PII was maintained on the Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.
>
> **Illinois Sub-Class**: All persons in the State of Illinois whose PII was maintained on the Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

The Nationwide Class and two state Sub-Classes are collectively referred to as the "Classes."

71. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from

this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

72. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

73. **Numerosity, Rule 23(a)(1):** The Classes are so numerous that joinder of all members is impracticable. Defendant has identified thousands of customers whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

74. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

75. **Commonality, Rule 23(a)(2) and (b)(3):** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include, but are not limited to, the following:

(a) Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

(b) Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

(c) Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

(d) Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

(e) Whether and when Defendant learned of the Data Breach;

(f) Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised; Whether Defendant violated its common law duties to Plaintiffs and Class Members by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

(g) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(h) Whether Defendant adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

(i) Whether Plaintiffs and Class Members are entitled to actual damages and/or punitive damages as a result of Defendant's wrongful conduct; Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

(j) Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach;

(k) Whether Defendant's data security systems prior to the Data Breach met the requirements of applicable laws and regulations;

(l) Whether Defendant's data security systems prior to the Data Breach met industry standards;

(m) Whether Plaintiffs' and other Class Members' PII was compromised in the Data Breach; and

(n) Whether Plaintiffs and other Class Members are entitled to damages as a result of Defendant's conduct.

76. **Typicality, Rule 23(a)(3):** Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance. Plaintiffs suffered the same injury as Class Members—i.e., upon information and belief, Plaintiffs' PII was compromised in the Data Breach.

77. **Ascertainability:** The Classes are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. The Classes consist of individuals who provided their PII to Samsung. Class Membership can be determined using Samsung's records and investigation.

78. **Policies Generally Applicable to the Classes:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class

Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

79. **Adequacy, Rule 23(a)(4):** Plaintiffs will fairly and adequately represent and protect the interests of the Classes. Plaintiffs have retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests that are contrary to or that conflict with those of the proposed Classes. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members.

80. Defendant has engaged in a common course of conduct toward Plaintiffs and other Class Members. The common issues arising from this conduct that affect Plaintiffs and Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

81. **Superiority and Manageability, Rule 23(b)(3):** A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendant. Concentrating this litigation in this forum is desirable to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendant's records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove the Plaintiffs' claims and the Class Members' claims.

82. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs

of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

83. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

84. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

85. A class action is appropriate under Rule 23(b)(2) because Defendant has acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

86. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the

resolution of which would advance the disposition of this matter and the parties' interests. These particular issues include, but are not limited to:

(a) Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

(b) Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

(c) Whether Defendant breached its own policies and applicable laws, regulations, and industry standards relating to data security;

(d) Whether Defendant adequately, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

(e) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

(f) Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

CLAIMS FOR RELIEF

COUNT I

Negligence
(On Behalf of Plaintiffs and the Classes)

87. Plaintiffs re-allege and incorporate all of the allegations contained in the preceding paragraphs.

88. To access features of the devices, application or service that Plaintiffs and Class Members purchased, Samsung required Plaintiffs and Class Members to submit certain PII, including their names, dates of birth, email addresses and mailing addresses.

89. Plaintiffs and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

90. By collecting and storing this PII and using it for commercial gain, Samsung has both a duty of care to use reasonable means to secure and safeguard this PII to prevent disclosure and guard against theft of the PII.

91. Defendant knows of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

92. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using its customers' PII involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

93. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and Class Members' information in Defendant's possession was adequately secured and protected.

94. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

95. Defendant's duty of care arose as a result of, among other things, the special relationship that existed between Samsung and its customers. Defendant was in a position to ensure that the PII of Plaintiffs and Class Members was secure and that it was safeguarding and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

96. Defendant was subject to an "independent duty," untethered to any contract between Samsung and Plaintiffs or Class Members.

97. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable to Defendant, particularly in light of Defendant's inadequate security practices and previous breach incidents.

98. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class Members, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

99. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth here. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' PII, including basic encryption techniques freely available to Defendant.

100. Plaintiffs and the Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

101. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

102. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs

and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

103. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

104. Defendant has admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

105. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within Defendant's possession or control.

106. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

107. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect customers' PII in the face of increased risk of theft.

108. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its customers' PII.

109. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

110. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

111. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

112. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to:

(a) actual identity theft;

(b) the loss of the opportunity of how their PII is used;

(c) the compromise, publication, and/or theft of their PII;

(d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

(f) costs associated with placing freezes on credit reports;

(g) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers in its continued possession;

(h) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the rest of the lives of Plaintiffs and Class Members; and

(i) the diminished value of Defendant's goods and services that Plaintiffs and Class Members received.

113. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

COUNT II

Invasion of Privacy
(On Behalf of Plaintiffs and the Classes)

114. Plaintiffs re-allege and incorporate all of the allegations contained in the preceding paragraphs.

115. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

116. Defendant owed a duty to its customers, including Plaintiffs and Class Members, to keep their PII contained and, as a part thereof, confidential.

117. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiffs and Class Members.

118. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and Class Members, through Defendant's failure to protect the PII.

119. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members is highly offensive to a reasonable person.

120. The intrusion was into a place or thing that was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Defendant as part

of their use of Defendant's services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

121. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

122. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with knowledge that its information security practices were inadequate and insufficient.

123. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

124. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

125. Unless enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs

and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT III

Negligence *Per Se*
(On Behalf of Plaintiffs and the Classes)

126. Plaintiffs re-allege and incorporate all of the allegations contained in the preceding paragraphs.

127. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

128. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the

immense damages that would result to Plaintiffs and Class Members due to the valuable nature of the PII at issue.

129. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

130. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

131. The harm that resulted from the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class Members.

132. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to,

(a) actual identity theft;

(b) the loss of the opportunity to control how their PII is used;

(c) the compromise, publication, or theft of their PII;

(d) out-of-pocket expenses associated with the prevention and detection of and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

(f) costs associated with placing freezes on credit reports;

(g) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession;

(h) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the rest of the lives of Plaintiffs and Class Members; and

(i) the diminished value of Defendant's goods and services Plaintiffs and Class Members received.

133. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT IV

Unjust Enrichment
(On Behalf of Plaintiffs and the Classes)

134. Plaintiffs re-allege and incorporate all of the allegations contained in the preceding paragraphs.

135. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transactions and should have been entitled to have Defendant protect their PII with adequate data security.

136. Defendant knew that Plaintiffs and Class Members conferred a benefit on Defendant and have accepted or retained that benefit. Defendant profited from the purchases and used the PII of Plaintiffs and Class Members for business purposes.

137. The amounts Plaintiffs and Class Members paid for Defendant's goods and services should have been used, in part, to pay for the administrative costs of data management and security, including the proper and safe disposal of Plaintiffs' and Class Members' PII.

138. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement the data management and security measures that are mandated by industry standards.

139. Defendant failed to secure the PII of Plaintiffs and Class Members and thus did not provide full compensation for the benefit Plaintiffs and Class Members provided.

140. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

141. If Plaintiffs and Class Members knew that Defendant would not secure their PII using adequate security, they would not have made purchases or provided their PII to Defendant.

142. Plaintiffs and Class Members have no adequate remedy at law.

143. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to,

(a) actual identity theft;

(b) the loss of the opportunity to determine how their PII is used;

(c) the compromise, publication, or theft of their PII;

(d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

(f) costs associated with placing freezes on credit reports;

(g) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession;

(h) future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the rest of the lives of Plaintiffs and Class Members; and

(i) the diminished value of Defendant's goods and services Plaintiffs and Class Members received.

144. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

145. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from Plaintiffs and Class Members. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's goods and services.

COUNT V

Violation of O.C.G.A. § 13-6-11
(On behalf of Plaintiffs, the Nationwide Class and the Georgia Sub-Class)

146. Plaintiffs re-allege and incorporate all of the allegations contained in the preceding paragraphs.

147. Defendant through its actions alleged and described herein acted in bad faith, was stubbornly litigious, or caused Plaintiffs unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

148. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to implement and use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

149. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal and sensitive data and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of personal and sensitive data it obtained and stored and the foreseeable consequences of a data breach.

150. Defendant also has a duty under the Georgia Constitution which contains a Right to Privacy clause, Chapter 1, Article 1, to protect its users' private

information. The Georgia Constitution states, "no person shall be deprived of life, liberty, or property except by due process of law." Moreover, the Georgia Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

151. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) §652A which specifically recognized four common law invasion of privacy claims in Georgia, which include 1) appropriation of likeness; 2) intrusion on solitude or seclusion; 3) public disclosure of private facts; and 4) false light.

152. Defendant's implementation of inadequate data security measures, its failure to resolve known vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required users to provide and stored on its own servers and databases constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

153. Defendant knew or should have known that it had a responsibility to protect the consumer data it required users to provide, that it was entrusted with this data, and that it was the only entity capable of adequately protecting the data on its systems and databases.

154. Despite that knowledge, Defendant abdicated its duty to protect the data it solicited and stored.

155. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to,

(a) actual identity theft;

(b) the loss of the opportunity to determine how their PII is used;

(c) the compromise, publication, or theft of their PII;

(d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

(f) costs associated with placing freezes on credit reports;

(g) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession;

(h) future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the rest of the lives of Plaintiffs and Class Members; and

(i) the diminished value of Defendant's goods and services Plaintiffs and Class Members received.

156. Plaintiffs therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

COUNT VI

Violation of the Illinois Consumer Fraud Act, 815 ILCS §§ 505, *et seq*.
(On Behalf of Plaintiffs. the Nationwide Class, and the Illinois Sub-Class)

157. Plaintiffs re-allege and incorporate all of the allegations contained in the preceding paragraphs.

158. This claim is brought under the laws of Illinois and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

159. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

160. Plaintiffs and Class Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

161. Defendant's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

162. Defendant's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' PII, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' PII, including duties imposed by the FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

(f) Failing to timely and adequately notify clients, Plaintiffs, and Class Members of the Data Breach;

(g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII;

(h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a); and

(i) By failing to provide disclose the Data Breach in a timely fashion, in violation of 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

163. Defendant's representations and omissions were material because they were likely to deceive reasonable clients and consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

164. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and Class Members, into believing that their clients' or their PII would not be exposed to unauthorized parties.

165. Defendant intended to mislead its customers, Plaintiffs, and Class Members, and induce them to rely on its misrepresentations and omissions.

166. The above unfair and deceptive practices and acts by Defendant offend public policy. These acts caused substantial injury that these consumers

could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

167. Defendant acted intentionally and knowingly to violate Illinois' Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Class Members' rights.

168. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to,

(a) actual identity theft;

(b) the loss of the opportunity to determine how their PII is used;

(c) the compromise, publication, or theft of their PII;

(d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

(f) costs associated with placing freezes on credit reports;

(g) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession;

(h) future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the rest of the lives of Plaintiffs and Class Members; and

(i) the diminished value of Defendant's goods and services Plaintiffs and Class Members received.

169. Plaintiffs and Class Members seek all monetary and non–monetary relief allowed by law, including damages, restitution, nominal and punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT VII

Violation of the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS §§ 510/2, *et seq.*
(On Behalf of Plaintiffs, the Nationwide Class, and the Illinois Sub-Class)

170. Plaintiffs re-allege and incorporate all of the allegations contained in the preceding paragraphs.

171. This claim is brought under the laws of Illinois and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

172. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

173. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

(a) Representing that goods or services have characteristics that they do not have;

(b) Representing that goods or services are of a particular standard, quality, or grade if they are of another;

(c) Advertising goods or services with intent not to sell them as advertised; and

(d) Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

174. Defendant's deceptive trade practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security

Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

(f) Failing to timely and adequately notify Plaintiffs and Class Members of the Data Breach;

(g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII;

(h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

175. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of Plaintiffs' and Class Members' PII.

176. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and Class Members, into believing that their PII would not be exposed to unauthorized parties.

177. The above unfair and deceptive practices and acts by Defendant offend and violate public policy. These acts caused substantial injury to Plaintiffs

and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

178. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to,

(a) actual identity theft;

(b) the loss of the opportunity to determine how their PII is used;

(c) the compromise, publication, or theft of their PII;

(d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

(f) costs associated with placing freezes on credit reports;

(g) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession;

(h) future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the rest of the lives of Plaintiffs and Class Members; and

(i) the diminished value of Defendant's goods and services Plaintiffs and Class Members received.

179. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class(es) proposed in this Complaint, respectfully request the Court enter judgment in their favor and against Defendant as follows:

a. For an Order certifying the Class(es), as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class, or in the alternative the separate Georgia and Illinois Sub-Classes;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the Data Breach and access and acquisition of Plaintiffs' and Class Members' PII by an unauthorized party, and from failing to issue prompt disclosures to Plaintiffs and Class Members;

c. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to PII collection, storage, maintenance, analysis, use, and protection;

d. A mandatory injunction directing Defendant to adequately safeguard Plaintiffs' and Class Members' PII by implementing improved security procedures and measures; specifically:

i. Requiring Defendant to protect, including through encryption, all data collected, maintained, and analyzed through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

ii. Requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and the Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class Members;

iii. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII;

iv. Prohibiting Defendant from maintaining Plaintiffs' and Class Members' PII on a cloud-based database;

v. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. Requiring Defendant to conduct regular database scanning and security checks;

x. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting Plaintiffs' and Class Members' PII;

xi. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xiii. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. Requiring Defendant to meaningfully educate all Class Members about the threats they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xv. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvi. For a period of 10 years, appointing a qualified and independent third-party assessor to conduct a System and Organization Controls ("SOC") 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xvii. Requiring Defendant to design, maintain, and test its computer systems to ensure PII in its possession is adequately secured and protected;

xviii. Requiring Defendant to disclose any future data breaches in a timely and accurate manner;

xix. Requiring Defendant to implement multi–factor authentication requirements;

xx. Requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxi. Requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class Members.

e. An award of other declaratory, injunctive, and equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

f. An award of restitution; compensatory, consequential, and general damages to Plaintiffs and Class Members, including nominal damages as allowed by law in an amount to be determined at trial or by this Court;

g. An award of actual or statutory damages to Plaintiffs and Class Members in an amount to be determined at trial or by this Court;

h. An award of reasonable litigation expenses and costs and attorneys' fees to the extent allowed by law;

i. An award of pre– and post–judgment interest to Plaintiffs and Class Members, to the extent allowable; and

j. Award such other and further relief as equity and this Court may deem just and proper.

k. Certification of the action as a Class Action pursuant to Federal Rule of Civil Procedure 23 and appointment of Plaintiffs as Class Representative and their counsel of record as Class Counsel;

l. That the acts alleged herein be adjudged and decreed to constitute negligence and violate the consumer protection laws of the States of Illinois and Georgia;

m. A judgment against Defendant for the damages sustained by Plaintiffs and the Classes defined here, and for any additional damages, penalties, and other monetary relief provided by applicable law;

n. An award to Plaintiffs and Class Members of pre-judgment and post-judgment interest as provided by law, and at the highest legal rate from and after service of the Complaint;

o. The costs of this suit, including reasonable attorneys' fees; and

p. Any other relief that the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs request a trial by jury on all issues so triable.

NOTICE TO THE ILLINOIS ATTORNEY GENERAL

A copy of this Complaint will be mailed to the Illinois Attorney General.

Dated January 18, 2023

Respectfully submitted,

/s/ Charles H. Van Horn

Charles H. Van Horn (GA Bar No. 724710)
Katherine M. Silverman (GA Bar No. 395741)
Carson L. Modrall (GA Bar No. 451366)
BERMAN FINK VAN HORN PC
3475 Piedmont Road, NE
Suite 1640
Atlanta, GA 30305
Telephone: (404) 261-7711
Facsimile: (404) 233-1943
cvanhorn@bfvlaw.com
ksilverman@bfvlaw.com
cmodrall@bfvlaw.com

Karen Hanson Riebel (MN #0219770)
Kate M. Baxter-Kauf (MN #0392037)
Arielle S. Wagner (MN#0398332)
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Avenue South
Suite 2200
Minneapolis, MN 55401
Telephone: (612) 596-4097
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
aswagner@locklaw.com
Counsel for Plaintiff